## REMARKS

Claims 1-25 are pending in the application - claims 1, 10, 18 and 24 are in independent form. Claims 1, 3-10, 12-18 and 20-25 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,926,546 ("Maeda et al."). Claims 2, 11 and 19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Maeda in view of U.S. Patent No. 6,631,271 ("Logan").

Applicants request traversal of these rejections and allowance of the pending claims in view of the following remarks.

Applicants' invention is directed to methods and system for authentication of communication units in a communications network. As recited in claim 1 for example, a method of granting, to a user communications device, access to a service provided by a plurality of service communications devices comprises: initiating a first communications link between the user communications device and a first one of a plurality of service communications devices, generating an access key code and storing a first data item indicating the access key code in a first storage means of the user communications device. The access key code is indicative of the user communications device and the service.

The method also includes making the access key code available to at least a second one of the plurality of service communications devices via a communications network, initiating a second communications link between the user communications device and the second service communications device and using the access key code to mutually authenticate the user communications device and the second service communications device.

Maeda discloses a toll collection system that includes a vehicle mounted device and a roadside device. These devices communicate data related to toll payment. A crypto module in the vehicle mounted device encrypts data submitted to the roadside device and decrypts data received from the roadside device.

The portions of Maeda relied upon for teaching access key code generation (i.e. col. 7, lines 34-42; col. 12, lines 1-15 and col. 12 lines 1-15 and col. 12, line 66 to col. 13, line 19) all describe the generation of encryption keys within the vehicle mounted device. Maeda does not disclose the generation of an access key code upon initiation of a communication link between a user communication device and one of a plurality of service communications devices. That is, the generation of encryption keys within the vehicle mounted device is independent of establishing a communication link between the devices.

As described in Maeda (col. 3, lines 20-25), and in contrast to Applicants' invention, data from vehicle mounted device is encrypted before the vehicle enters the communication area of the roadside device; therefore, a communication link is not established between the vehicle mounted device and the roadside device until after the data is encrypted for transmission from the vehicle mounted device. In Applicants' invention, as recited further in claims 10, 18 and 24, communication link is established and an access key code is generated during an initialization procedure of the first communications link.

The code generated in Maeda (col. 6, lines 4-22) is not indicative of the user communications device and the service – it indicates toll payment information.

Maeda also fails to disclose the making the access key available to a second '

communications device. Maeda describes communication of encrypted data and not the communication of an access key code (col. 7, lines 44-49).

Furthermore, Maeda fails to teach the use of the generated access key code to mutually authenticate the user communications device and the second communications device. The communication between the vehicle mounted device and the roadside device takes place in an unconditional and unauthenticated manner as the data is transferred upon detection of a pilot signal; that is, it takes place without prior mutual authentication. The data may be encrypted in Maeda but it is encrypted before the vehicle enters the communication area of the roadside device. If the vehicle has not entered the communication area of the roadside device, the vehicle will not be able to communicate with the roadside device. The verification in Maeda relates to verifying the IC card and the encryptor within the vehicle communications device (col. 4, lines 33-50) and verifying the IC card and the crypto module within the vehicle communications device (col. 13, lines 50-55).

As Maeda fails to teach or disclose each element in claim 1 of Applicants' invention, the rejection of claim 1 as being anticipated by Maeda should be withdrawn. At least for these reasons, it is respectfully submitted that claim 1 is allowable over the teachings of Maeda.

The deficiencies of Maeda as highlighted above also apply equally to the remaining independent claims (i.e. claims 10, 18 and 24). Therefore, claims 10, 18 and 24 are also allowable over the teachings of Maeda. The teachings of Logan fail to overcome the deficiencies of Maeda described above. The remaining claims (i.e. 2-9, 11-17, 19-23 and 25), all depending on one of the allowable independent claims, are also allowable.

Application No. 10/005,080
Docket No. 0119-141

It is respectfully submitted that this application is in condition for allowance and a notice to that effect is earnestly solicited. Should the Examiner have any questions with respect to expediting the prosecution of this application, she is urged to contact the undersigned at the number listed below.

Respectfully submitted,

Potomac Patent Group, PLLC

By: _____
Kris Kalidindi
Reg. No. 41,461

Date: December 3, 2004

Potomac Patent Group PLLC
P.O. Box 0855
McLean, VA 22101-0855
703-905-9818